Writing representations over proper sub-division rings

S. P. GLASBY

Abstract. Let $\mathbb{E}$ be a division ring and G a finite group of automorphisms of $\mathbb{E}$ whose elements are distinct modulo inner automorphisms of $\mathbb{E}$. Given a representation $\rho\colon \mathfrak{A} \to \mathrm{GL}_d(\mathbb{E})$ of an $\mathbb{F}$-algebra $\mathfrak{A}$, we give necessary and sufficient conditions for ρ to be *writable* over $\mathbb{F} = \mathbb{E}^G$, i.e. whether or not there exists a matrix A in $\mathrm{GL}_d(\mathbb{E})$ that conjugates $\rho(\mathfrak{A})$ into $\mathrm{GL}_d(\mathbb{F})$. We give an algorithm for constructing an A, or proving that no A exists. The case of particular interest to us is when $\mathbb{E}$ is a field, and ρ is absolutely irreducible. The algorithm relies on an explicit formula for A, and a generalization of Hilbert's Theorem 90 (Theorem 3) that arises in Galois cohomology. The algorithm has applications to the construction of absolutely irreducible group representations (especially for solvable groups), and to the recognition of one of the classes in Aschbacher's matrix group classification scheme.

Keywords: Hilbert's Theorem 90, proper sub-division ring

2000 Mathematics subject classification: 20C40, 20C10

1. Introduction

Throughout this paper $\mathbb{E}$ denotes a division ring, G a finite group of automorphisms of $\mathbb{E}$ whose elements are distinct modulo inner automorphisms of $\mathbb{E}$, and $\mathbb{F} = \mathbb{E}^G$ is the sub-division ring fixed elementwise by G. In the second half of this paper, we shall specialize to the case when $\mathbb{E} : \mathbb{F}$ is a finite Galois extension of *fields*. We view $\mathrm{GL}_d(\mathbb{E})$ as the group of invertible $d \times d$ matrices over $\mathbb{E}$. We say that a representation $\rho\colon \mathfrak{A} \to \mathrm{GL}_d(\mathbb{E})$ of an $\mathbb{F}$-algebra $\mathfrak{A}$ *can be written over* $\mathbb{F}$ if there exists an $A \in \mathrm{GL}_d(\mathbb{E})$ such that

$$A^{-1}\rho(x)A \in \mathrm{GL}_d(\mathbb{F}) \qquad (x \in \mathfrak{A}).$$

The purpose of this paper is threefold: (1) to describe the connection between Galois cohomology and the problem of writing ρ over $\mathbb{F}$, (2) to describe properties of a map Π_C used to construct A, and (3) to give an algorithm that takes as input an absolutely irreducible ρ and either constructs an A, or proves that no such A exists.

Date: Draft printed on February 1, 2008.

Section 2 describes briefly how A gives rise to a certain function $C\colon G \to \mathrm{GL}_d(\mathbb{E})$ called 1-cocycle. The more interesting problem of how C gives rise to A is discussed in Section 3. The heart of this problem involves a generalization of Hilbert's Theorem 90: there exists a matrix $A \in \mathrm{GL}_d(\mathbb{E})$ such that $C_\alpha = A\alpha(A)^{-1}$ for $\alpha \in G$. Equivalently, using the language of Galois cohomology, it says that $H^1(G, \mathrm{GL}_d(\mathbb{E})) = \{I\}$. This result was proved by Serre [16] when $\mathbb{E}$ is a field, and by Nuss [11] when $\mathbb{E}$ is a division ring. Neither the proof by Serre nor Nuss is constructive: both proofs require modification in order to suggest an algorithm. We shall give a completely elementary proof in Theorem 3 of these results which suggests both a deterministic and a probabilistic algorithm for constructing A. Although some of our results can be rephrased in terms of Galois cohomology [16], and descent theory for noncommutative rings [11], we prefer to state our results with minimal background in terms of matrices over $\mathbb{E}$ and automorphisms.

Given a 1-cocycle $C\colon G \to \mathrm{GL}_d(\mathbb{E})$, we can construct an endomorphism $\Pi_C\colon \mathbb{E}^{d\times d} \to \mathbb{E}^{d\times d}$ of the algebra of $d \times d$ matrices over $\mathbb{E}$. In Sections 3 and 4 we focus on properties of Π_C. If X is a random element of $\mathbb{E}^{d\times d}$, then the probability that $A = \Pi_C(X)$ writes ρ over $\mathbb{F}$ is at least $\prod_{i=1}^{\infty}(1 - 2^{-i}) > 2/7$. After Theorem 8 we shall assume that $\mathbb{E}$ is a (commutative) field. Different choices for X can give different choices for A, and a random X can be a poor choice e.g. the entries of A may be 100 digit integers. We show in Theorem 10 that if $\mathbb{E}$ is a field and $|\mathbb{F}| \geq d$, then we may take X to be a scalar matrix. This result, which is best possible, appears to be helpful in producing "nice" conjugating matrices A. Furthermore, whether $\lambda \in \mathbb{E}$ or $X \in \mathbb{E}^{d\times d}$, it appears that the probabilities $\mathrm{Prob}(\Pi_C(\lambda I)$ invertible) and $\mathrm{Prob}(\Pi_C(X)$ invertible) are very close.

Section 5 focuses on the case when ρ is an absolutely irreducible representation. In this case we construct a map $D\colon G \to \mathrm{GL}_d(\mathbb{E})$ and seek a function $\mu\colon G \to \mathbb{E}^\times$ such that μD is a 1-cocycle. The existence of μ determines whether or not ρ can be written over $\mathbb{F}$. If $\mathbb{E}$ is a cyclotomic number field, then the existence of μ depends on the solutions to certain equations in $\mathbb{E}$. We solve, if possible, certain norm equations, and then solve equations in the group of units of the ring of algebraic integers of $\mathbb{E}$.

Section 6 discusses some simple Las Vegas algorithms primarily for computing $(q-1)$th roots, and solving norm equations in finite fields. Section 7 gives examples arising from representations of groups. Although our results apply to arbitrary $\mathbb{F}$-algebras $\mathfrak{A}$, the examples presented have $\mathfrak{A} = \mathbb{F}H$ where $\mathbb{F}H$ is a group algebra of a not necessarily finite group H. If $\sigma\colon H \to \mathrm{GL}_d(\mathbb{E})$ is a group representation, then σ

may be extended, via a familiar argument, to a representation ρ of the group algebra $\mathfrak{A} = \mathbb{F}H$. Of course, ρ can be written over $\mathbb{F}$ precisely when σ can. The existence of a normal basis for $\mathbb{E}$ over $\mathbb{F}$ plays an important role in Section 7 and in Theorem 10.

Our work has been influenced by [4], which considers the case when G is cyclic, and by Brückner's PhD thesis [1]. In [1] Brückner independently discovers some results in [4], and describes an unpublished result due to Plesken [1, Satz 3] which gives a necessary and sufficient condition for an absolutely irreducible group representation over a field $\mathbb{E}$ to be writable over $\mathbb{F}$ where $\mathbb{E} : \mathbb{F}$ is a finite Galois extension of fields. An algorithm is given in [1, Lemma 7] for writing ρ over $\mathbb{F}$ when G is cyclic. The proof contains errors, however, all may be corrected. It involves choosing a random column vector $x \in \mathbb{E}^{d\times 1}$ rather than choosing a random matrix $X \in \mathbb{E}^{d\times d}$. This viewpoint motivated our Proposition 5.

In the sequel we will denote automorphisms of $\mathbb{E}$ by α, β, γ, elements of $\mathbb{E}$ by λ, μ, ν, and representations of $\mathfrak{A}$ by ρ, ρ', σ.

2. From A to C_α

We shall say that ρ *can be written over* $\mathbb{F}$ if there exists an $A \in \mathrm{GL}_d(\mathbb{E})$ such that

$$A^{-1}\rho(x)A \in \mathrm{GL}_d(\mathbb{F}) \qquad (x \in \mathfrak{A}).$$

Our goal is to construct a conjugating matrix A, or prove that one does not exist.

An automorphism $\alpha \in \mathrm{Aut}(\mathbb{E})$ induces an automorphism, also denoted α, of the algebra $\mathbb{E}^{d\times d}$ of $d \times d$ matrices over $\mathbb{E}$: $(\mu_{i,j}) \mapsto (\alpha(\mu_{i,j}))$. Now A writes ρ over $\mathbb{F}$ if and only if

$$\alpha(A^{-1}\rho(x)A) = A^{-1}\rho(x)A \qquad (x \in \mathfrak{A}, \alpha \in G).$$

In subsequent equations, which hold for all $x \in \mathfrak{A}$, we shall omit the x's and simply write

$$\alpha(A^{-1}\rho A) = A^{-1}\rho A \qquad (\alpha \in G). \tag{1}$$

Therefore $C_\alpha := A\alpha(A)^{-1}$ satisfies

$$C_\alpha^{-1}\rho\, C_\alpha = \alpha \circ \rho \qquad (\alpha \in G). \tag{2}$$

Furthermore, $A\alpha\beta(A)^{-1} = A\alpha(A)^{-1}\alpha(A\beta(A)^{-1})$ and so

$$C_{\alpha\beta} = C_\alpha \alpha(C_\beta) \qquad (\alpha, \beta \in G). \tag{3}$$

We chose our automorphisms to act on the left, to avoid the "twisted" equation $C_{\alpha\beta} = C_\beta(C_\alpha)^\beta$, which follows from $C_\alpha = A(A^\alpha)^{-1}$.

A map $C\colon G \to \mathrm{GL}_d(\mathbb{E})$ defined by $\alpha \mapsto C_\alpha$ satisfying Eq. (3) is called a *1-cocycle*, and if there exists an $A \in \mathrm{GL}_d(\mathbb{E})$ such that $C_\alpha = A\alpha(A)^{-1}$ for all $\alpha \in G$, then C is called a *1-coboundary*. In summary, a necessary condition for ρ to be writable over $\mathbb{F}$ is that there exist a 1-cocycle C satisfying Eq. (2). More significantly, a 1-cocycle C is a 1-coboundary, by a generalization of Hilbert's Theorem 90, and there exist constructive methods for finding A from C, and hence for writing ρ over $\mathbb{F}$.

3. From C_α to A

The following result generalizes a well-known result of Artin [10, VIII §4, Theorem 7] which says that distinct characters $H \to \mathbb{E}^\times$ of a group H with values in a field $\mathbb{E}$, are linearly independent over $\mathbb{E}$.

Lemma 1. *Let $\mathbb{E}$ be a division ring.*

(a) *Let $\chi_1, \dots, \chi_n$ be group homomorphisms $H \to \mathbb{E}^\times$ which are distinct modulo inner automorphisms of $\mathbb{E}$. Then $\chi_1, \dots, \chi_n$ are linearly independent over $\mathbb{E}$.*

(b) *If G is a finite subgroup of $\mathrm{Aut}(\mathbb{E})$ whose elements are distinct modulo $\mathrm{Inn}(\mathbb{E})$, then the trace map $\mathrm{Tr}\colon \mathbb{E} \to \mathbb{F}\colon \lambda \mapsto \sum_{\alpha\in G}\alpha(\lambda)$ is surjective.*

Proof. (a) We shall view $\mathbb{E}$ as a left vector space over $\mathbb{F}$. The proof can be modified for right $\mathbb{F}$-spaces. Suppose that $\lambda_1\chi_1 + \cdots + \lambda_n\chi_n = 0$ where not all λ_i are zero, and n is positive and minimal. Then $n \geq 2$ and each λ_i is nonzero. If $h, k \in H$, then

$$\lambda_1\chi_1(k) + \cdots + \lambda_n\chi_n(k) = 0,$$
$$\lambda_1\chi_1(hk) + \cdots + \lambda_n\chi_n(hk) = 0.$$

Premultiplying the first equation by $\lambda_1\chi_1(h)\lambda_1^{-1}$ and subtracting the second equation gives $\sum_{i=2}^{n}\left(\lambda_1\chi_1(h)\lambda_1^{-1}\lambda_i - \lambda_i\chi_i(h)\right)\chi_i(k) = 0$ for all $h, k \in H$. The minimality of n implies that each coefficient is zero. Therefore $\chi_i(h) = \lambda_i^{-1}\lambda_1\chi_1(h)\lambda_1^{-1}\lambda_i$ for all $h \in H$, and χ_i is equivalent modulo $\mathrm{Inn}(\mathbb{E})$ to χ_1 for $i \geq 2$, a contradiction.

(b) Let $\chi_1, \dots, \chi_n$ denote the elements of G and let $H = \mathbb{E}^\times$. By part (a), $\chi_1, \dots, \chi_n$ are $\mathbb{E}$-linearly independent and hence $\sum_{\alpha\in G}\alpha \neq 0$. Therefore the $\mathbb{F}$-linear map $\mathrm{Tr}\colon \mathbb{E} \to \mathbb{F}$ is surjective. □

Assume we know matrices $C_\alpha \in \mathrm{GL}_d(\mathbb{E})$ satisfying Eq. (3). Theorem 3 shows how to construct $A \in \mathrm{GL}_d(\mathbb{E})$ such that $C_\alpha = A\alpha(A)^{-1}$ for $\alpha \in G$. It relies on the following simple lemma.

Lemma 2. *Let $\mathbb{E}$ be a division ring, and let G be a finite subgroup of* $\mathrm{Aut}(\mathbb{E})$.

(a) *If* $C_\alpha \in \mathbb{E}^{d\times d}$ *satisfies* $C_{\alpha\beta} = C_\alpha + \alpha(C_\beta)$ *for all* $\alpha, \beta \in G$, *then* $\Pi_C(X) = \sum_{\alpha\in G} C_\alpha + \alpha(X)$ *satisfies* $C_\alpha + \alpha(\Pi_C(X)) = \Pi_C(X)$ *for all* $X \in \mathbb{E}^{d\times d}$ *and* $\alpha \in G$.

(b) *If* $C_\alpha \in \mathrm{GL}_d(\mathbb{E})$ *satisfies Eq. (3), then* $\Pi_C(X) = \sum_{\alpha\in G} C_\alpha\alpha(X)$ *satisfies* $C_\alpha\alpha(\Pi_C(X)) = \Pi_C(X)$ *for all* $X \in \mathbb{E}^{d\times d}$ *and* $\alpha \in G$.

(c) *If* $C_\alpha \in \mathrm{GL}_d(\mathbb{E})$ *satisfies Eq. (3) and no two elements of* G *are equal modulo* $\mathrm{Inn}(\mathbb{E})$, *then then there exists a* $\lambda \in \mathbb{E}$ *such that the first column,* x, *of* $\Pi_C(I\lambda)$ *is nonzero, and satisfies* $C_\alpha\alpha(x) = x$ *for all* $\alpha \in G$.

Proof. We omit the proof of part (a) as it follows from the proof of part (b) with products replaced by sums. It follows from Eq. (3) that

$$C_\alpha\alpha(\Pi_C(X)) = C_\alpha\alpha\left(\sum_{\beta\in G} C_\beta\beta(X)\right) = \sum_{\alpha\in G} C_{\alpha\beta}\alpha\beta(X) = \Pi_C(X).$$

Consider part (c). Let e be the column vector with 1 in the first row, and zeroes elsewhere. Then $x = \Pi_C(I\lambda)e$, and by part (b)

$$C_\alpha\alpha(x) = C_\alpha\alpha(\Pi_C(I\lambda)e) = C_\alpha\alpha(\Pi_C(I\lambda))e = \Pi_C(I\lambda)e = x.$$

Moreover, each of the column vectors of $C_\alpha\alpha(\lambda)$ are nonzero. By Lemma 1(b) the elements of G are $\mathbb{E}$-linearly independent. Hence there exists a $\lambda \in \mathbb{E}$ such that $x = \sum_{\alpha\in G} C_\alpha\alpha(\lambda)e \neq 0$. ☐

The sum $\sum C_\alpha\alpha(X)$ was considered in [4]. I have learned recently that this sum dates back to Poincaré [16, p. 159]. I attribute the following theorem to Serre [16, Prop. 3] when $\mathbb{E}$ is a field, and to Nuss [11, Theorem B] when $\mathbb{E}$ is a division ring. We offer an elementary proof conducive to practical implementation. A discussion of non-matrix versions of Hilbert's Theorem 90 over division rings can be found in [9].

Theorem 3. *Let* $\mathbb{E}$ *be a division ring and* G *a finite subgroup of* $\mathrm{Aut}(\mathbb{E})$ *whose elements are distinct modulo* $\mathrm{Inn}(\mathbb{E})$.

(a) *Let* $C_\alpha \in \mathbb{E}^{d\times d}$, $\alpha \in G$. *There exists an* $A \in \mathbb{E}^{d\times d}$ *satisfying* $C_\alpha = A - \alpha(A)$, $\alpha \in G$, *if and only if* $C_{\alpha\beta} = C_\alpha + \alpha(C_\beta)$ *for all* $\alpha, \beta \in G$.

(b) *Let* $C_\alpha \in \mathrm{GL}_d(\mathbb{E})$, $\alpha \in G$. *There exists an* $A \in \mathrm{GL}_d(\mathbb{E})$ *satisfying* $C_\alpha = A\alpha(A)^{-1}$, $\alpha \in G$, *if and only if* $C_{\alpha\beta} = C_\alpha\alpha(C_\beta)$ *for all* $\alpha, \beta \in G$.

Proof. The forward implication is straightforward for parts (a) and (b). The reverse implication follows from Lemma 2 for part (a), and for part (b) *provided* there exists and $X \in \mathbb{E}^{d\times d}$ such that $\Pi_C(X)$ is

invertible. While it is clear that the image of Π_C contains *nonzero* matrices, it is more subtle that $\mathrm{im}(\Pi_C)$ contains *invertible* matrices. We prove this second fact via induction on d.

The result is true when $d = 1$ by Lemma 2(c) since if $x \neq 0$, then the 1×1 matrix $[x]$ is invertible. Suppose that $d > 1$ and that the result is true for dimension $d - 1$. By Lemma 2(c) there exists an invertible matrix Y with first column x, satisfying $C_\alpha \alpha(x) = x$ for all $\alpha \in G$. Therefore,

$$Y^{-1}C_\alpha \alpha(Y) = \begin{pmatrix} 1 & y_\alpha \\ 0 & C'_\alpha \end{pmatrix} \qquad (\alpha \in G)$$

where $C'_\alpha \in \mathrm{GL}_{d-1}(\mathbb{E})$. Since $Y^{-1}C_\alpha\alpha(Y)$ satisfies Eq. (3), so too does C'_α. By induction, there exists an $A' \in \mathrm{GL}_{d-1}(\mathbb{E})$ satisfying $C'_\alpha \alpha(A') = A'$ for all $\alpha \in G$. Thus

$$\begin{pmatrix} 1 & 0 \\ 0 & A' \end{pmatrix}^{-1} Y^{-1}C_\alpha\alpha(Y)\alpha\begin{pmatrix} 1 & 0 \\ 0 & A' \end{pmatrix} = \begin{pmatrix} 1 & z_\alpha \\ 0 & I \end{pmatrix} =: C''_\alpha \qquad (\alpha \in G).$$

Since C''_α satisfies Eq. (3), the z_α satisfy $z_{\alpha\beta} = z_\alpha + \alpha(z_\beta)$ for all $\alpha, \beta \in G$. By part (a) there exists a $1 \times (d-1)$ vector w such that $z_\alpha = w - \alpha(w)$ for all $\alpha \in G$. Therefore, $A = Y\begin{pmatrix} 1 & 0 \\ 0 & A' \end{pmatrix}\begin{pmatrix} 1 & w \\ 0 & I \end{pmatrix}$. $\square$

Lemma 2(b) entreats us to study the maps $\Pi_C, \Gamma_\alpha \colon \mathbb{E}^{d\times d} \to \mathbb{E}^{d\times d}$ defined by

$$\Pi_C(X) = \sum_{\alpha\in G} C_\alpha\alpha(X) \quad \text{and} \quad \Gamma_\alpha(X) = C_\alpha\alpha(X) - X.$$

When $\mathrm{char}(\mathbb{E}) \nmid |G|$, it is convenient to also define π_C by $\pi_C = |G|^{-1}\Pi_C$. The matrix A in Theorem 3 satisfying $C_\alpha = A\alpha(A)^{-1}$ is far from unique. Indeed the matrix AY, where $Y \in \mathrm{GL}_d(\mathbb{F})$, has the same property. It is useful to regard $\mathbb{E}^{d\times d}$ as a right $\mathbb{F}^{d\times d}$-module, where the scalar action is right matrix multiplication.

Proposition 4. *Let $C \colon G \to \mathrm{GL}_d(\mathbb{E})$ be a 1-cocycle where $\mathbb{E}$ is a division ring and G is a finite subgroup of* $\mathrm{Aut}(\mathbb{E})$.

(a) *The maps Π_C and Γ_α are right $\mathbb{F}^{d\times d}$-homomorphisms satisfying $\Pi_C \circ \Gamma_\alpha = \Gamma_\alpha \circ \Pi_C = 0$ and $\Pi_C^2 = |G|\Pi_C$.*
(b) *If $\mathrm{char}(\mathbb{E}) \nmid |G|$, then $\pi_C^2 = \pi_C$ and so $\mathbb{E}^{d\times d} = \mathrm{im}(\pi_C) \dotplus \ker(\pi_C)$ where $\ker(\pi_C) = \mathrm{im}(1 - \pi_C)$. Moreover, if $\pi_C(X) = XY$ where $Y \in \mathrm{GL}_d(\mathbb{F})$, then $\pi_C(X) = X$.*
(c) *If $C_\alpha = A\alpha(A)^{-1}$ for all $\alpha \in G$, then $\Pi_C(X) = A\mathrm{Tr}(A^{-1}X)$ where $\mathrm{Tr} \colon \mathbb{E}^{d\times d} \to \mathbb{F}^{d\times d}$ is the trace function: $X \mapsto \sum_{\alpha\in G}\alpha(X)$. Moreover, $\Pi_C(A\lambda) = A\mathrm{Tr}(\lambda)$, $\Pi_C(A) = |G|A$ and $\pi_C(A) = A$.*

(d) *Let* $Y \in \mathrm{GL}_d(\mathbb{E})$ *be fixed, and let* $D\colon G \to \mathrm{GL}_d(\mathbb{E})$ *be defined by* $D_\alpha = Y^{-1}C_\alpha\alpha(Y)$*. Then* D_α *satisfies* Eq. (3)*, and*

$$\Pi_D(X) = Y^{-1}\Pi_C(YX).$$

Proof. (a) It is clear that $\Pi_C(X_1 + X_2) = \Pi_C(X_1) + \Pi_C(X_2)$ and $\Pi_C(XY) = \Pi_C(X)Y$ for all $Y \in \mathbb{F}^{d\times d}$. Thus Π_C, and similarly Γ_α, are right $\mathbb{F}^{d\times d}$-module homomorphisms. Lemma 2(b) shows that $\Gamma_\alpha \circ \Pi_C = 0$, and the following argument shows that $\Pi_C \circ \Gamma_\beta = 0$:

$$\Pi_C(C_\beta\beta(X)) = \sum_{\alpha\in G} C_\alpha\alpha(C_\beta\beta(X)) = \sum_{\alpha\in G} C_{\alpha\beta}\alpha\beta(X) = \Pi_C(X).$$

In addition, by the above equation:

$$\Pi_C^2(X) = \sum_{\beta\in G} \Pi_C(C_\beta\beta(X)) = \sum_{\beta\in G} \Pi_C(X) = |G|\Pi_C(X).$$

(b) Multiplying the equation $\Pi_C^2 = |G|\Pi_C$ by $|G|^{-2}$ gives $\pi_C^2 = \pi_C$. Standard arguments show that $\mathbb{E}^{d\times d} = \mathrm{im}(\pi_C) \dotplus \ker(\pi_C)$. If $\pi_C(X)$ equals XY, then by part (a)

$$XY = \pi_C(X) = \pi_C^2(X) = \pi_C(XY) = \pi_C(X)Y = XY^2.$$

Postmultiplying by Y^{-1} gives $X = XY$. Thus $\pi_C(X) = X$.

Consider part (c):

$$\Pi_C(X) = \sum_{\alpha\in G} A\alpha(A)^{-1}\alpha(X) = A\sum_{\alpha\in G} \alpha(A^{-1}X) = A\mathrm{Tr}(A^{-1}X).$$

Setting $X = A\lambda$ shows $\Pi_C(A\lambda) = A\mathrm{Tr}(I\lambda) = A\mathrm{Tr}(\lambda)$, and setting $\lambda = 1$ shows $\Pi_C(A) = |G|A$ and $\pi_C(A) = A$. Part (d) is straightforward. (The 1-cocycles C and D are called *cohomologous*.) $\square$

The endomorphisms Π_C, Γ_α of $\mathbb{E}^{d\times d}$ give rise to endomorphisms $\widehat{\Pi}_C$, $\widehat{\Gamma}_\alpha$ of the space $\mathbb{E}^{d\times 1}$ of $d \times 1$ column vectors:

$$\widehat{\Pi}_C(x) = \sum_{\alpha\in G} C_\alpha\alpha(x), \quad \widehat{\Gamma}_\alpha(x) = C_\alpha\alpha(x) - x \qquad (\alpha \in G).$$

When $\mathrm{char}(\mathbb{E}) \nmid |G|$, it is convenient to also define $\widehat{\pi}_C$ by $\widehat{\pi}_C = |G|^{-1}\widehat{\Pi}_C$. If $x \in \mathbb{E}^{d\times 1}$ is the first column of $X \in \mathbb{E}^{d\times d}$, and $Y = \mathrm{diag}(1, 0, \dots, 0)$, then the first columns of $\Pi_C(XY) = \Pi_C(X)Y$ and $\Gamma_\alpha(XY) = \Gamma_\alpha(X)Y$ are $\widehat{\Pi}_C(x)$ and $\widehat{\Gamma}_\alpha(x)$ respectively.

It is worth recording some simple generalizations of Prop. 4(a,b,c) such as: $\widehat{\Gamma}_\alpha \circ \widehat{\Pi}_C = \widehat{\Pi}_C \circ \widehat{\Gamma}_\alpha = 0$, $\widehat{\Pi}_C^2 = |G|\widehat{\Pi}_C$, $\mathbb{E}^{d\times 1} = \mathrm{im}(\widehat{\pi}_C) \dotplus \ker(\widehat{\pi}_C)$ and $\widehat{\Pi}_C(x) = A\mathrm{Tr}(A^{-1}x)$ where Tr denotes the trace map $\mathbb{E}^{d\times 1} \to \mathbb{F}^{d\times 1}$.

Proposition 5. *Let $C\colon G \to \mathrm{GL}_d(\mathbb{E})$ be a 1-cocycle where $\mathbb{E}$ is a division ring and G is a finite subgroup of $\mathrm{Aut}(\mathbb{E})$ whose elements are distinct modulo $\mathrm{Inn}(\mathbb{E})$. Let S be a generating set for G, and let $\mathbb{F} = \mathbb{E}^G$.*

(a) $\mathrm{im}(\widehat{\Pi}_C) = \bigcap_{\alpha\in S}\ker(\widehat{\Gamma}_C)$ *is the $\mathbb{F}$-linear span of the columns of any matrix A satisfying $C_\alpha = A\alpha(A)^{-1}$ for all $\alpha \in G$.*

(b) *If $\mathrm{char}(\mathbb{E}) \nmid |G|$, then $\ker(\widehat{\Pi}_C) = \sum_{\alpha\in S}\mathrm{im}(\widehat{\Gamma}_\alpha)$.*

(c) *If $\alpha \neq 1$, then $\mathrm{im}(\widehat{\Gamma}_\alpha)$ spans $\mathbb{E}^{d\times 1}$ as an $\mathbb{E}$-space.*

(d) *If $0 \neq x \in \ker(\widehat{\Pi}_C)$, then $x\mathbb{E} \not\subseteq \ker(\widehat{\Pi}_C)$.*

Proof. (a) $\widehat{\Gamma}_\alpha \circ \widehat{\Pi}_C = 0$, implies $\mathrm{im}(\widehat{\Pi}_C) \subseteq \bigcap_{\alpha\in S}\ker(\widehat{\Gamma}_\alpha)$. Conversely, if $x \in \bigcap_{\alpha\in S}\ker(\widehat{\Gamma}_\alpha)$, then $C_\alpha\alpha(x) = x$ for $\alpha \in S$. It follows from Eq. (3) that $C_\alpha\alpha(x) = x$ for $\alpha \in G$. Thus

$$\Pi_C(x\lambda) = \sum_{\alpha\in G} C_\alpha\alpha(x)\alpha(\lambda) = \sum_{\alpha\in G} x\alpha(\lambda) = x\mathrm{Tr}(\lambda).$$

By Lemma 1(b), there exists a $\lambda \in \mathbb{E}$ such that $\mathrm{Tr}(\lambda) = 1$. Thus $x \in \mathrm{im}(\widehat{\Pi}_C)$ and so $\mathrm{im}(\widehat{\Pi}_C) = \bigcap_{\alpha\in S}\ker(\widehat{\Gamma}_\alpha)$. It follows from Prop. 4(c) that $\mathrm{im}(\widehat{\Pi}_C) = A\mathbb{F}^{d\times d}$, and so $\mathrm{im}(\widehat{\Pi}_C)$ is the $\mathbb{F}$-linear span of columns of A.

(b) $\widehat{\Pi}_C \circ \widehat{\Gamma}_\alpha = 0$, implies $\ker(\widehat{\Pi}_C) \supseteq \sum_{\alpha\in S}\mathrm{im}(\widehat{\Gamma}_\alpha)$. It follows from Eq. (3) that

$$C_{\alpha\beta}\alpha\beta(x) - x = [C_\alpha\alpha(C_\beta\beta(x)) - C_\beta\beta(x)] + [C_\beta\beta(x) - x].$$

Hence $\mathrm{im}(\widehat{\Gamma}_{\alpha\beta}) \subseteq \mathrm{im}(\widehat{\Gamma}_\alpha) + \mathrm{im}(\widehat{\Gamma}_\beta)$ and $\sum_{\alpha\in G}\mathrm{im}(\widehat{\Gamma}_\alpha) = \sum_{\alpha\in S}\mathrm{im}(\widehat{\Gamma}_\alpha)$. Conversely, if $x \in \ker(\widehat{\Pi}_C)$, then $\sum_{\alpha\in G} C_\alpha\alpha(x) = 0$ and hence

$$x = \mathrm{Tr}(|G|^{-1}x) = \sum_{\alpha\in G}\widehat{\Gamma}_\alpha(|G|^{-1}x) \in \sum_{\alpha\in G}\mathrm{im}(\widehat{\Gamma}_\alpha) = \sum_{\alpha\in S}\mathrm{im}(\widehat{\Gamma}_\alpha).$$

Thus $\ker(\widehat{\Pi}_C) = \sum_{\alpha\in S}\mathrm{im}(\widehat{\Gamma}_\alpha)$ as desired.

(c) Suppose that Let $\phi\colon \mathbb{E}^{d\times 1} \to \mathbb{E}$ be an $\mathbb{E}$-linear map containing $\mathrm{im}(\widehat{\Gamma}_\alpha)$ in its kernel. Then for all $x \in \mathbb{E}^{d\times 1}$ and $\lambda \in \mathbb{E}$:

$$0 = \phi(\widehat{\Gamma}_\alpha(x\lambda)) = \phi(C_\alpha\alpha(x))\alpha(\lambda) - \phi(x)\lambda.$$

Since $\alpha \neq 1$ it follows from Lemma 1(a) that $\phi(x) = 0$ for all x and hence $\phi = 0$. This proves that the $\mathbb{E}$-linear span of $\mathrm{im}(\widehat{\Gamma}_\alpha)$ equals $\mathbb{E}^{d\times 1}$, and hence $\dim_{\mathbb{F}}(\mathrm{im}(\widehat{\Gamma}_\alpha)) \geq d$.

(d) Suppose that $0 \neq x \in \ker(\widehat{\Pi}_C)$. If $\widehat{\Pi}_C(x\lambda) = 0$ for all $\lambda \in \mathbb{E}$, then $\sum_{\alpha\in G} C_\alpha\alpha(x)\alpha(\lambda) = 0$. Since $C_\alpha\alpha(x) \neq 0$, this contradicts Lemma 1(a). Thus $x\mathbb{E} \not\subseteq \ker(\widehat{\Pi}_C)$ as claimed. □

In light of Prop. 5(a) the assumption in Prop. 5(b) that $\mathrm{char}(\mathbb{E}) \nmid |G|$ may be unnecessary.

Proposition 6. *Let $(\lambda_\alpha)_{\alpha \in G}$ be an $\mathbb{F}$-basis for $\mathbb{E}$, and let $E_{i,j} \in \mathbb{E}^{d\times d}$ be the matrix with 1 in the (i,j)th entry and zeroes elsewhere. Then $\mathbb{E}^{d\times d}$ is a freely generated as a right $\mathbb{F}^{d\times d}$-module by $E_{i,1}\lambda_\alpha$, $\alpha \in G$, $i = 1, \dots, d$.*

Proof. By taking $\mathbb{F}$-linear combinations of $E_{i,1}\lambda_\alpha$ gives a matrix with arbitrary first column. Taking $\mathbb{F}^{d\times d}$-multiples gives every element of $\mathbb{E}^{d\times d}$. The fact that the $E_{i,1}\lambda_\alpha$ freely generate $\mathbb{E}^{d\times d}$ follows from the observation that $E_{i,1}\mathbb{F}^{d\times d}$ comprises matrices with all rows zero except the ith, and the ith row can be an arbitrary vector in $\mathbb{F}^{1\times d}$. □

It follows from Theorem 3 and the above proposition that an invertible matrix can be found by taking $\mathbb{F}^{d\times d}$-linear combinations of the matrices $\Pi_C(\lambda_\alpha E_{i,1})$. Since each $\Pi_C(\lambda_\alpha E_{i,1})$ is singular (unless $d = 1$), it is better to consider $\mathbb{F}^{d\times d}$-linear combinations of $\Pi_C(\lambda_\alpha D^i)$ where D is the permutation matrix corresponding to the d-cycle $(1, 2, \dots, d)$. A simple argument shows that the $\lambda_\alpha D^i$ generate $\mathbb{E}^{d\times d}$ as a $\mathbb{F}^{d\times d}$-module, although not freely. In practice $\mathbb{F}^{d\times d}$-linear combinations are not necessary as $\Pi_C(\lambda_\alpha D^i)$ is commonly invertible. Thus we typically do not evaluate $\Pi_C(X)$ at a random matrix X. Doing so can result in "bad" matrices $A = \Pi_C(X)$, e.g. with 100 digit integer entries. More significantly, the matrices $A^{-1}\rho(x)A$ can be "bad". Choosing X to be a scalar matrix seems to result in "good" matrices $\Pi_C(X)$. This imprecise statement has some theoretical underpinning in Theorem 10.

4. Invertible elements in $\mathrm{im}(\Pi_c)$

The primary aim of this section is to prove in Theorem 10 that if $|\mathbb{F}| \geq d$ there exists a $\lambda \in \mathbb{E}$ such that $\Pi_C(I\lambda)$ is invertible. We show in Theorem 8 that the assumption $|\mathbb{F}| \geq d$ is best possible by considering a special case when A, and hence each C_α, is upper-triangular.

We need a preliminary lemma.

Lemma 7. *Let V be a vector space over a division ring $\mathbb{F}$. If V is a union of m proper subspaces, then $\dim_{\mathbb{F}}(V) \geq 2$ and $|\mathbb{F}| < m$. Conversely, if $\dim_{\mathbb{F}}(V) \geq 2$ and $\mathbb{F}$ is finite, then V is a union of $|\mathbb{F}|+1$ proper subspaces.*

Proof. The proof in [6, Problem 24] generalizes to division rings. If $\dim_{\mathbb{F}}(V) \geq 2$, then $V = H_\infty \cup \bigcup_{\lambda \in \mathbb{F}} H_\lambda$ where H_∞ is the hyperplane $x_1 = 0$ and H_λ the hyperplane $\lambda x_1 + x_2 = 0$. Thus V is a union of $|\mathbb{F}| + 1$ proper subspaces. □

Theorem 8. *Let $C\colon G \to \mathrm{GL}_d(\mathbb{E})$ be a 1-cocycle where G and $\mathbb{E}$ are as in Theorem 3. Suppose that $C_\alpha = A\alpha(A)^{-1}$, $\alpha \in G$, where $A \in \mathrm{GL}_d(\mathbb{E})$ is upper-triangular and $\mathbb{F} = \mathbb{E}^G$. If $|\mathbb{F}| \geq d$, then there exists a $\lambda \in \mathbb{E}$ such that $\Pi_C(I\lambda)$ is invertible. Moreover, if $|\mathbb{F}| < d$, then there exists an upper-triangular matrix $A \in \mathrm{GL}_d(\mathbb{E})$ such that $\Pi_C(I\lambda)$ is singular for all $\lambda \in \mathbb{E}$.*

Proof. It follows from Prop. 4(c) that $\Pi_C(I\lambda)$ is invertible if and only if $\mathrm{Tr}(A^{-1}\lambda)$ is invertible. If $a_{i,i}$ denotes the (i,i)th entry of A, then $\mathrm{Tr}(A^{-1}\lambda)$ is upper-triangular with (i,i)th entry $\mathrm{Tr}(a_{i,i}^{-1}\lambda)$. Let $K(a_{i,i}^{-1})$ denote the kernel of the map $\lambda \mapsto \mathrm{Tr}(a_{i,i}^{-1}\lambda)$. By Lemma 1(b) the $\mathbb{F}$-subspace $K(a_{i,i}^{-1})$ of $\mathbb{E}$ has codimension 1. If $|\mathbb{F}| \geq d$, then $\mathbb{E}$ is not a union of d proper subspaces by Lemma 7. Thus there exists a $\lambda \in \mathbb{E}$ not in $\bigcup_{i=1}^d K(a_{i,i}^{-1})$. Since $\mathrm{Tr}(a_{i,i}^{-1}\lambda) \neq 0$ for each i, it follows that $\Pi_C(I\lambda)$ is invertible.

Conversely, suppose that $|\mathbb{F}| < d$. Then $\mathbb{E}$ is a union of $|\mathbb{F}| + 1$ proper subspaces, so we may choose $a_{1,1}^{-1}, \dots, a_{d,d}^{-1} \in \mathbb{E}^\times$ such that $\mathbb{E} = \bigcup_{i=1}^d K(a_{i,i}^{-1})$. Then for each $\lambda \in \mathbb{E}$ at least one diagonal entry of the upper-triangular matrix $\mathrm{Tr}(A^{-1}\lambda)$ is zero. Put differently, $\Pi_C(I\lambda)$ is singular for all $\lambda \in \mathbb{E}$. □

Assumption: We shall henceforth assume that $\mathbb{E}$ is a *field*.

Theorem 10 generalizes Theorem 8 to deal with arbitrary $d \times d$ matrices A. Its proof assumes that $\mathbb{E}$ is a field, and depends on the following well-known result.

Lemma 9. *Let f be an element of the polynomial ring $\mathbb{F}[x_1, \dots, x_n]$ such that $f(a_1, \dots, a_n) = 0$ for all $(a_1, \dots, a_n) \in \mathbb{F}^n$.*

(a) *If the degree of f in each variable is less than $|\mathbb{F}|$, then $f = 0$.*
(b) *If the degree of f is at most q where $|\mathbb{F}| = q$, then there exists $\nu_1, \dots, \nu_n \in \mathbb{F}$ such that $f(x_1, \dots, x_n) = \sum_{i=1}^n \nu_i(x_i^q - x_i)$.*

Proof. (a) See [10, Chapter V, Theorem 5] (and [10, Corollary 3]) for the case when $\mathbb{F}$ is finite (and $\mathbb{F}$ is infinite). Consider part (b). Recall that the degree of a nonzero polynomial is the maximum degree of a monomial summand, and $\deg(x_1^{k_1} \cdots x_n^{k_n}) = k_1 + \cdots + k_n$. The result is true when $n = 1$. Suppose that $n > 1$ and $f = \sum_{i=0}^q f_i x_n^{q-i}$ where f_i is a polynomial in $x_1, \dots, x_{n-1}$ of degree at most i. Fix $(a_1, \dots, a_{n-1}) \in \mathbb{F}^{n-1}$ and consider $f(a_1, \dots, a_{n-1}, x^n)$. By the $n = 1$ case, $f_i(a_1, \dots, a_{n-1}) = 0$ for $i = 1, \dots, q-2$ and $f_0 = -f_{q-1} = \nu_n$ is a constant polynomial. By part (a), $f_i = 0$ for $i = 1, \dots, q-2$ and by induction there exist $\nu_1, \dots, \nu_{n-1} \in \mathbb{F}$ such that $f_q = \sum_{i=1}^{n-1} \nu_i(x_i^q - x_i)$. In summary, $f = \sum_{i=1}^n \nu_i(x_i^q - x_i)$. □

The reader may like to compare Lemma 9(b) with a theorem due to Chevalley [15, §1.7, Theorem 2].

Theorem 10. *Let $\mathbb{E}$ be a field, and $\mathbb{E} : \mathbb{F}$ a finite Galois extension with group G. Suppose that $C\colon G \to \mathrm{GL}_d(\mathbb{E})$ is a 1-cocycle and $|\mathbb{F}| \geq d$. Then there exists a $\lambda \in \mathbb{E}$ such that $\Pi_C(I\lambda) = \sum_{\alpha\in G} C_\alpha \alpha(\lambda)$ is invertible.*

Proof. By Theorem 3 there exists an invertible matrix A satisfying $C_\alpha = A\alpha(A)^{-1}$, $\alpha \in G$. By Prop. 4(c), $\Pi_C(\lambda I) = A\mathrm{Tr}(\lambda A^{-1})$. Thus $\Pi_C(\lambda I)$ is invertible precisely when $\mathrm{Tr}(\lambda A^{-1})$ is invertible. Our problem can be rephrased: Given $X \in \mathrm{GL}_d(\mathbb{E})$, find $\lambda \in \mathbb{E}$ such that $\mathrm{Tr}(\lambda X)$ is invertible.

By [14, Theorems 7.4.2, 8.7.2] there exists $\zeta \in \mathbb{E}$ such that $(\alpha(\zeta))_{\alpha\in G}$ is a basis for $\mathbb{E}$ over $\mathbb{F}$ (such a basis is called a *normal basis*). Now $\mathrm{Tr}(\zeta) \in \mathbb{F}^\times$ by Lemma 1(b). By replacing ζ by $\mathrm{Tr}(\zeta)^{-1}\zeta$ we may additionally assume that $\mathrm{Tr}(\zeta) = 1$. A typical element of $\mathbb{E}$ has the form $\sum_{\alpha\in G} x_\alpha \alpha(\zeta)$ where $x_\alpha \in \mathbb{F}$. Write

$$x_{i,j} = \sum_{\alpha\in G} x^{i,j}_\alpha \alpha(\zeta) \quad \text{and} \quad \lambda = \sum_{\beta\in G} \lambda_\beta \beta(\zeta)$$

where $x_{i,j}$ denotes the (i,j)th entry of X. We shall view the $x^{i,j}_\alpha$ as *elements* of $\mathbb{F}$, and the λ_β as algebraically independent commuting *variables* that are fixed by G.

Let $(\mu_{\alpha,\beta})$ be the matrix of the $\mathbb{F}$-linear transformation $\mathbb{E} \to \mathbb{E}$ defined by $\lambda \mapsto \zeta\lambda$. That is,

$$\zeta\alpha(\zeta) = \sum_{\beta\in G} \mu_{\alpha,\beta}\beta(\zeta) \qquad (\mu_{\alpha,\beta} \in \mathbb{F}). \tag{4}$$

Then

$$\begin{aligned} x\lambda &= \left(\sum_\alpha x_\alpha \alpha(\zeta)\right)\left(\sum_\beta \lambda_\beta \beta(\zeta)\right) = \sum_{\alpha,\beta} x_\alpha \lambda_\beta \alpha(\zeta\alpha^{-1}\beta(\zeta)) \\ &= \sum_{\alpha,\beta,\gamma} x_\alpha \lambda_\beta \mu_{\alpha^{-1}\beta,\gamma}\ \alpha\gamma(\zeta). \end{aligned}$$

Replacing $\alpha\gamma$ by γ gives $x\lambda = \sum x_\alpha \lambda_\beta \mu_{\alpha^{-1}\beta,\alpha^{-1}\gamma}\ \gamma(\zeta)$. Our normalization implies that $\mathrm{Tr}(\gamma(\zeta)) = 1$, and hence

$$\mathrm{Tr}(x\lambda) = \sum_\alpha \left(\sum_{\beta,\gamma} \mu_{\alpha^{-1}\beta,\alpha^{-1}\gamma}\lambda_\beta\right) x_\alpha. \tag{5}$$

Abbreviate the above inner sum by z_α. Then

$$\begin{aligned} z_\alpha &= \sum_\beta \left(\sum_\gamma \mu_{\alpha^{-1}\beta,\alpha^{-1}\gamma} \right) \lambda_\beta = \sum_\beta \mathrm{Tr}(\zeta\alpha^{-1}\beta(\zeta))\lambda_\beta \\ &= \sum_\beta \mathrm{Tr}(\alpha(\zeta)\beta(\zeta))\lambda_\beta. \end{aligned} \tag{6}$$

Replacing x_α in Eq. (5) by $x_\alpha^{i,j}$ shows

$$\det \mathrm{Tr}(X\lambda) = \det(x_{i,j}\lambda) = \det\left(\sum_\alpha z_\alpha x_\alpha^{i,j}\right).$$

This determinant is a polynomial in the variables z_α which is either the zero polynomial, or is homogeneous of degree d in the z_α. Specifically,

$$\det\left(\sum_\alpha z_\alpha x_\alpha^{i,j}\right) = \sum p_{\{\alpha_1,\dots,\alpha_d\}} z_{\alpha_1} \cdots z_{\alpha_d} \tag{7}$$

where the sum is taken over all orbits of the symmetric group S_d on the group G^d. Such orbits are in bijective correspondence with the multisets $\{\alpha_1, \dots, \alpha_d\}$ of G having at least one, and at most d, distinct elements. We view the coefficient $p_{\{\alpha_1,\dots,\alpha_d\}}$ of $z_{\alpha_1} \cdots z_{\alpha_d}$ as an element of $\mathbb{F}$, not a polynomial over $\mathbb{F}$ in the $x_\alpha^{i,j}$.

The matrix $(\mathrm{Tr}(\alpha(\zeta)\beta(\zeta)))_{\alpha,\beta\in G}$ is invertible (see [14, §7.2]), and its determinant equals the discriminant $\prod_{\alpha\neq\beta}(\alpha(\zeta)-\beta(\zeta))$ of the minimal polynomial $\prod_\alpha(t-\alpha(\zeta))$ of ζ over $\mathbb{F}$. By Eq. (6) as (λ_β) runs through the vectors in the vector space $\mathbb{F}^{|G|}$, (z_α) does the same.

The determinant $\det(X) = \det(\sum_\alpha x_\alpha^{i,j}\alpha(\zeta))$ can be evaluated using the same reasoning used for Eq. (7). Replacing z_α by $\alpha(\zeta)$ in Eq. (7) shows

$$\det(X) = \sum p_{\{\alpha_1,\dots,\alpha_d\}} \alpha_1(\zeta) \cdots \alpha_d(\zeta). \tag{8}$$

Let us assume that X is fixed and that $\det \mathrm{Tr}(X\lambda) = 0$ for all $\lambda \in \mathbb{E}$ (or equivalently, all $(\lambda_\beta) \in \mathbb{F}^{|G|}$). By virtue of the previous paragraph, this says that the polynomial Eq. (7) is zero for all $(z_\alpha) \in \mathbb{F}^{|G|}$. If $|\mathbb{F}| > d$, then Lemma 9(a) implies that each $p_{\{\alpha_1,\dots,\alpha_d\}}$ equals zero. By Eq. (8), $\det(X) = 0$. In summary, we have proved that if $|\mathbb{F}| > d$ and $\det(X) \neq 0$, then there exists a $\lambda \in \mathbb{E}$ such that $\det \mathrm{Tr}(\lambda X) \neq 0$.

Finally, suppose that $|\mathbb{F}| = d$ is finite and $\det \mathrm{Tr}(X\lambda) = 0$ for all $\lambda \in \mathbb{E}$. By Lemma 9(b), $\det \mathrm{Tr}(X\lambda) = \sum_{\alpha\in G} \nu_\alpha(z_\alpha^{|\mathbb{F}|} - z_\alpha)$. Since this polynomial is not homogeneous, each ν_α is zero. Thus each $p_{\{\alpha_1,\dots,\alpha_d\}}$ equals zero, and $\det(X) = 0$ by Eq. (8). This completes the proof. $\square$

In the light of Theorem 8, one may suspect that Theorem 10 holds more generally: namely when $\mathbb{E}$ is a division ring.

5. Algorithmic considerations

Henceforth assume that $\rho\colon \mathfrak{A} \to \mathrm{GL}_d(\mathbb{E})$ is an *absolutely irreducible* representation, and $\langle S \mid R\rangle$ is a finite presentation of G.

If ρ can be written over $\mathbb{F}$, then there exist matrices $D_\alpha \in \mathrm{GL}_d(\mathbb{E})$ satisfying

$$D_\alpha^{-1}\rho D_\alpha = \alpha \circ \rho \qquad\qquad (\alpha \in G). \tag{9}$$

There are a variety of methods for calculating the D_α, or proving that some do not exist. These include (a) using the Meataxe algorithm [8, 13], (b) solving $d^2|G|$ homogeneous linear equations over $\mathbb{F}$ in $d^2|G|$ unknowns, and (c) averaging over a chain $\mathfrak{A} = \mathfrak{A}_1 \supset \cdots \supset \mathfrak{A}_{n+1} = \{0\}$ of $\mathbb{F}$-algebras where the indices $|\mathfrak{A}_i : \mathfrak{A}_{i+1}|$ are "small".

If ρ can be written over $\mathbb{F}$, then by absolute irreducibility there exists a function $\mu\colon G \to \mathbb{E}^\times$ such that $C = \mu D$ is a 1-cocycle. It suffices to know C_α for $\alpha \in S$, because Eq. (3) allows us to compute C_γ for $\gamma \in G$. Suppose henceforth that we have computed matrices D_α, $\alpha \in S$, that satisfy Eq. (9). Now the C_α, $\alpha \in S$, satisfy the relations R for G, and in general the D_α will not. The relations give rise to a system of $|R|$ equations that the scalars μ_α must satisfy. If these equations can not be solved in $\mathbb{E}^\times$, then ρ can not be written over $\mathbb{F}$, otherwise it can by Section 2. We shall say more about the equations that the μ_α satisfy.

Two important applications of this work are (a) when $\mathbb{E}$ is a subfield of a cyclotomic field, and (b) when $\mathbb{E}$ is a finite field. In these cases G is abelian, or cyclic and we assume that G has a presentation:

$$G = \langle \alpha_1, \dots, \alpha_s \mid \alpha_i^{m_i} = 1, 1 \le i \le s, [\alpha_j, \alpha_i] = 1, 1 \le i < j \le s\rangle$$

where $[\alpha, \beta]$ denotes the commutator $\alpha^{-1}\beta^{-1}\alpha\beta$. We shall not necessarily assume that $m_1|m_2|\cdots|m_s$.

The power relations and the commutator relations give different equations that the μ_α must satisfy. Consider first relations of the form $\alpha^m = 1$. It follows from Eq. (3) that $C_{\alpha^m} = C_\alpha \alpha(C_\alpha)\cdots\alpha^{m-1}(C_\alpha)$ and hence that

$$\begin{aligned} D_\alpha\alpha(D_\alpha)\cdots\alpha^{m-1}(D_\alpha) &= \lambda_\alpha I \quad \text{where} \\ \mu_\alpha\alpha(\mu_\alpha)\cdots\alpha^{m-1}(\mu_\alpha) &= \lambda_\alpha^{-1} \qquad (\alpha \in S). \end{aligned} \tag{10}$$

Given a subgroup A of G, define the norm map $N_A\colon \mathbb{E}^\times \to (\mathbb{E}^A)^\times$ by $N_A(\lambda) = \prod_{\alpha\in A}\alpha(\lambda)$. Then Eq. (10) says: $N_{\langle\alpha\rangle}(D_\alpha) = \lambda_\alpha I$ where $N_{\langle\alpha\rangle}(\mu_\alpha) = \lambda_\alpha^{-1}$ for some $\mu_\alpha \in \mathbb{E}^\times$. A necessary condition is that $\alpha(\lambda_\alpha) = \lambda_\alpha$. When $\mathbb{E}$ is finite, $N_{\langle\alpha\rangle}$ is surjective, and this necessary

condition is sufficient to guarantee a solution for μ_α. By contrast, when $\mathbb{E}$ is infinite the equation $N_{\langle\alpha\rangle}(\mu_\alpha) = \lambda_\alpha^{-1}$ may have no solution (c.f. Section 7, Example 1). There are a variety of algorithms for solving for μ_α when $\mathbb{E}$ is finite, see for example Section 6. Different algorithms are required in the the case when $\mathbb{E}$ is a number field, see for example [2] and [17]. Assume henceforth that the equations $N_{\langle\alpha\rangle}(\mu_\alpha) = \lambda_\alpha^{-1}$ can be solved. By replacing D_α by $\mu_\alpha^{-1} D_\alpha$ we will henceforth assume that $\lambda_\alpha = 1$ for $\alpha \in S$. We shall now seek a function ν such that νD is a 1-cocycle.

Consider now equations arising from commutators $[\alpha, \beta] = 1$ where $\alpha, \beta \in S$. Applying Eq. (3) twice gives

$$C_\alpha \alpha(C_\beta) = C_{\alpha\beta} = C_{\beta\alpha} = C_\beta \beta(C_\alpha) \qquad (\alpha, \beta \in G).$$

Substituting $C_\alpha = \nu_\alpha D_\alpha$ into $\alpha(C_\beta)^{-1} C_\alpha^{-1} C_\beta \beta(C_\alpha) = I$ gives

$$\begin{aligned} \alpha(D_\beta)^{-1} D_\alpha^{-1} D_\beta \beta(D_\alpha) = \lambda_{\alpha,\beta} I \quad &\text{where} \\ \beta(\nu_\alpha)^{-1} \nu_\beta^{-1} \nu_\alpha \alpha(\nu_\beta) = \lambda_{\alpha,\beta} \qquad &(\alpha, \beta \in S). \end{aligned} \tag{11}$$

Let K_A and I_A denote the kernel and image of the norm map N_A. As we are assuming that $\lambda_\alpha = \lambda_\beta = 1$ it follows that $\nu_\alpha \in K_A$ and $\nu_\beta \in K_B$ where $A = \langle\alpha\rangle$ and $B = \langle\beta\rangle$. It follows from Eq. (11) that $N_A(\lambda_{\alpha,\beta}) = N_B(\lambda_{\alpha,\beta}) = 1$, and hence a necessary condition is that $\lambda_{\alpha,\beta} \in K_A \cap K_B$.

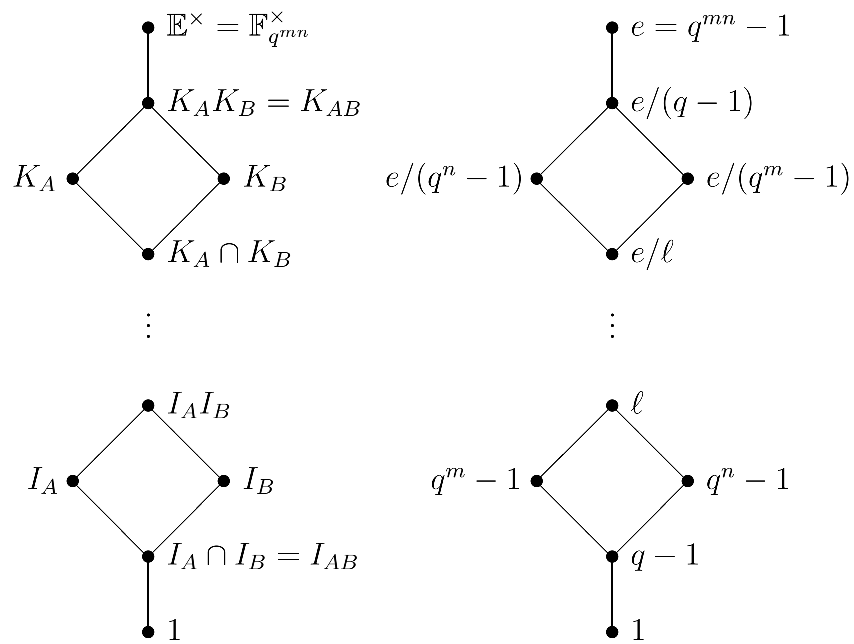

Figure 1. Subgroups of $\mathbb{F}_{q^{mn}}^\times$ and their orders.

Since $AB = BA$ and $A \cap B = 1$, N_{AB} equals $N_A \circ N_B = N_B \circ N_A$, and hence $K_A K_B \subseteq K_{AB}$ and $I_{AB} \subseteq I_A \cap I_B$. If $\mathbb{E}$ is finite, then these containments are equalities, and the necessary condition $\lambda_{\alpha,\beta} \in K_A \cap K_B$ is sufficient to solve Eq. (11) for $\nu_\alpha \in K_A$ and $\nu_\beta \in K_B$ (see Section 6).

When $\mathbb{F} = \mathbb{E}^{AB}$ is finite of order q, then $\mathbb{E} = \mathbb{F}_{q^{mn}}$, and $G = AB$. In Figure 1, $\ell = \gcd(q^m - 1, q^n - 1) = (q^m - 1)(q^n - 1)/(q - 1)$ and $I_{AB} = \mathbb{F}^\times$.

Suppose that $\mathbb{E}$ is a number field and ρ maps into $\mathrm{GL}_d(\mathbb{Z}_\mathbb{E})$, where $\mathbb{Z}_\mathbb{E}$ denotes the ring of integers of $\mathbb{E}$. Then there exist algorithms [3] for computing the group $U(\mathbb{Z}_\mathbb{E})$ of units of $\mathbb{Z}_\mathbb{E}$. Therefore solving

$$\beta(\nu_\alpha)^{-1}\nu_\beta^{-1}\nu_\alpha\alpha(\nu_\beta) = \lambda_{\alpha,\beta} \qquad (\alpha, \beta \in S)$$

for $\nu_\alpha \in K_{\langle\alpha\rangle}$, $\nu_\beta \in K_{\langle\beta\rangle}$ reduces to solving a linear system over $\mathbb{Z}$.

Although evaluating $\Pi_C(X)$ is clearly useful, it is time-consuming when $|G|$ is large unless an averaging argument is used. We describe how to use a subgroup chain $G = G_0 > G_1 > \cdots > G_{t+1} = 1$ to reduce the cost of computing $\Pi_C(X)$ from $\mathrm{O}(|G|)$ to $\mathrm{O}(\sum_{i=1}^t |G_{i-1} : G_i|)$. If $G = \alpha_1 H \cup \cdots \cup \alpha_r H$ is a decomposition of G into left cosets of H, then

$$\Pi_C(X) = \sum_{i=1}^r \sum_{\beta \in H} C_{\alpha_i\beta}\alpha_i\beta(X) = \sum_{i=1}^r C_{\alpha_i}\alpha_i \left(\sum_{\beta\in H} C_\beta \beta(X)\right).$$

Put differently, $\Pi_{C|G} = \sum_{i=1}^r C_{\alpha_i}\alpha_i\Pi_{C|H}$. If G is solvable, then we may choose G_i so that $G_i \triangleright G_{i+1}$ and $G_i = \langle\gamma_i, G_{i+1}\rangle$. In this case, an idea in [4, p. 1705] further reduces the complexity of evaluating $\Pi_C(X)$ to $\mathrm{O}(\log|G|)$.

6. Las Vegas algorithms

A Las Vegas algorithm is one that involves random choices, and when it terminates it produces an answer that is provably correct. For example, a 1-cocycle $C \colon G \to \mathrm{GL}_d(\mathbb{E})$ may be written as $C_\alpha = A\alpha(A)^{-1}$, $\alpha \in G$, by repeated selecting a random $X \in \mathbb{E}^{d\times d}$ until $A = \Pi_C(X)$ is invertible. If $|\mathbb{F}| = q$ is finite and a uniform distribution is used for $\mathbb{E}^{d\times d}$, then the probability that $\Pi_C(X)$ is invertible is

$$f(d,q) = \frac{|\mathrm{GL}_d(\mathbb{F})|}{|\mathbb{F}^{d\times d}|} = \prod_{i=1}^d (1 - q^{-i}).$$

Note that

$$\limsup_q f(d,q) = f(d,\infty) = 1 \quad \text{and} \quad \liminf_{d,q} f(d,q) = f(\infty,2).$$

The following bounds for $f(d,q)$ are useful:

$$1-q^{-1}\geq f(d,q)>\prod_{i=1}^{\infty}(1-q^{-i})>1-\sum_{i=1}^{\infty}q^{-i}=1-(q-1)^{-1}.$$

If $q=2$, then $f(\infty,2)=0.288788\cdots>2/7$ gives a better lower bound. Thus one would expect to make on average at most 3.5 choices for X. The probability that the algorithm fails to terminate after n selections is $(1-f(d,q))^n<\min\{(q-1)^{-n},(5/7)^n\}$. If $\mathbb{E}$ is infinite, then it follows by localization and a local-global argument that the probability that $\Pi_C(X)$ is invertible is 1.

In the light of Theorem 10 we should also consider the probability, p_C, that a random $\lambda\in\mathbb{E}^\times$ has $\Pi_C(\lambda I)$ invertible. If $\mathbb{E}$ is finite, then certain choices for C have $p_C=1$. Empirical evidence suggests that when $|\mathbb{E}|$ is small the average value of p_C, averaged over all 1-cocycles C, is a number very close to $f(d,q)$. This is our default expectation.

We describe a Las Vegas algorithm for computing $(q-1)$th roots. Let $C\colon G\to \mathrm{GL}_1(\mathbb{E})$ be a 1-cocycle where $\mathbb{E}=\mathbb{F}_{q^n}$, $\mathbb{F}=\mathbb{F}_q$ and $G=\langle\alpha\rangle$ where $\alpha(\lambda)=\lambda^q$. If $C_\alpha=\lambda$, then $\lambda\alpha(\lambda)\cdots\alpha^{n-1}(\lambda)=1$ and finding $\mu\in\mathbb{E}^\times$ such that $\lambda=\mu\alpha(\mu)^{-1}$ is equivalent to finding a $(q-1)$th root, as $\mu^{q-1}=\lambda^{-1}$. Lemma 2(b) gives a Las Vegas algorithm for computing μ: choose $\nu\in\mathbb{E}$ randomly until $\Pi_C(\nu)$ is nonzero. As Π_C is a nonzero $\mathbb{F}$-linear map $\mathbb{E}\to\mathbb{F}$, each ν has probability $1-q^{-1}$ of success. Unless q is small, this Las Vegas algorithm is faster than factoring the polynomial $x^{q-1}-\lambda^{-1}$ over $\mathbb{E}$.

We comment now on Las Vegas algorithms for solving norm equations in finite fields. Let $\mathbb{E}=\mathbb{F}_{q^n}$, $\mathbb{F}=\mathbb{F}_q$ and let $\lambda\in\mathbb{F}^\times$. Denote by e, f and $|\lambda|$ the orders of $\mathbb{E}^\times$, $\mathbb{F}^\times$ and $\langle\lambda\rangle$ respectively. One may solve the equation $N(\mu)=\lambda$ by randomly selecting $\nu\in\mathbb{E}^\times$ and checking whether or not $\mu=\nu^{f/|\lambda|}$ satisfies $N(\mu)=\lambda$. As the norm map $N\colon\mathbb{E}^\times\to\mathbb{F}^\times\colon\mu\mapsto\mu^{e/f}$ is surjective, each selection has probability $|\lambda|^{-1}$ of success. This algorithm is useful when $|\lambda|$ is small. If $|\lambda|$ is large, then another Las Vegas algorithm is more desirable. Let $d=\gcd(|\lambda|,e/f)$. Since $q\equiv 1\mod|\lambda|$, it follows that $e/f\equiv n \mod|\lambda|$. In most applications, n is small when f is large, and hence when $|\lambda|$ is large d is usually much smaller. Denote by s a multiplicative inverse of $e/(fd)$ modulo $|\lambda|/d$. Randomly select $\nu\in\mathbb{E}^\times$. A root μ of the polynomial $x^d-\lambda^s\nu^f$ has probability d^{-1} of satisfying $N(\mu)=\lambda$.

We prove that the above algorithm is correct, and that either all dth roots μ of $\lambda^s\nu^f$ satisfy $N(\mu)=\lambda$, or none do. Let $\mathbb{E}^\times=\langle\zeta\rangle$, and suppose that $\lambda=\zeta^{ie/f}$ and $\nu=\zeta^j$. As $\zeta^{e/f}$ has order f, $|\lambda|$ equals $f/\gcd(i,f)$. Let $r,s\in\mathbb{Z}$ satisfy $r|\lambda|+se/f=d$ where $d=\gcd(|\lambda|,e/f)$.

If $\mu = \zeta^k$, then modulo e

$$\begin{aligned} dk &\equiv ise/f + jf \\ &\equiv i(d - r|\lambda|) + jf \\ &\equiv id + (-t + j)f \quad \text{where } t := ir/\gcd(i, f) \in \mathbb{Z}. \end{aligned}$$

There exists an $\ell \in \mathbb{Z}$ such that

$$\begin{aligned} k &= i + (j - t)f/d + \ell e/d \\ ke/f &= ie/f + (j - t)e/d + \ell(e/d)(e/f) \\ &\equiv ie/f + (j - t)e/d \mod e. \end{aligned}$$

So $N(\mu) = N(\zeta^k) = \zeta^{ke/f} = \zeta^{ie/f}(\zeta^{e/d})^{j-t} = \lambda\omega^{j-t}$ where $\omega = \zeta^{e/d}$ has order d. In summary, $N(\mu) = \lambda$ if and only if $j \equiv t \mod d$. Thus the probability of success is d^{-1}. As the value of $N(\mu)$ is independent of ℓ, either each of the d roots μ satisfy $N(\mu) = \lambda$, or none do.

In the case when $\mathbb{E}$ is finite and $|G| = |\mathbb{E} : \mathbb{F}|$ is not a prime power, then a divide-and-conquer strategy may be used for solving norm equations. Suppose that $|\mathbb{E} : \mathbb{F}| = mn$ where $\gcd(m, n) = 1$ and $\mathbb{F} = \mathbb{F}_q$. Let $G = AB$ where $A = \langle\alpha\rangle$ satisfies $\alpha(\lambda) = \lambda^{q^n}$, and $B = \langle\beta\rangle$ satisfies $\beta(\lambda) = \lambda^{q^m}$. Then $|A| = m$ and $|B| = n$. If the presentation $G = \langle\alpha\beta \mid (\alpha\beta)^{mn} = 1\rangle$ is used, then one need only solve one norm equation: $\mu_{\alpha\beta}^{(q^{mn}-1)/(q-1)} = \lambda_{\alpha\beta}$ where $\lambda_{\alpha\beta} \in \mathbb{F}^\times$ is given. If the presentation $G = \langle\alpha, \beta \mid \alpha^m = \beta^n = [\beta, \alpha] = 1\rangle$ is used, then one must solve three equations: $\mu_\alpha^{(q^{mn}-1)/(q^n-1)} = \lambda_\alpha$, $\mu_\beta^{(q^{mn}-1)/(q^m-1)} = \lambda_\beta$ and $\nu_\alpha^{1-q^m}\nu_\beta^{q^n-1} = \lambda_{\alpha,\beta}$ where $\lambda_\alpha \in \mathbb{E}^A$, $\lambda_\beta \in \mathbb{E}^B$ and $\lambda_{\alpha,\beta} \in K_A \cap K_B$. The two norm equations could be solved using the above Las Vegas algorithm. This has the advantage that $\gcd(|\lambda_\alpha|, m)$ and $\gcd(|\lambda_\beta|, n)$ are likely smaller than $\gcd(|\lambda_{\alpha\beta}|, mn)$. There exist $r, s \in \mathbb{Z}$ such that

$$r(q^m - 1) + s(q^n - 1) = q - 1.$$

Since $\lambda_{\alpha,\beta} \in K_A \cap K_B \subseteq K_{AB}$, our Las Vegas algorithm for computing $(q-1)$th roots may be used to solve the equations $\nu_\alpha^{q-1} = \lambda_{\alpha,\beta}^{-r}$ and $\nu_\beta^{q-1} = \lambda_{\alpha,\beta}^s$. Then

$$\nu_\alpha^{1-q^m}\nu_\beta^{q^n-1} = \lambda_{\alpha,\beta}^{r(q^m-1)/(q-1)+s(q^n-1)/(q-1)} = \lambda_{\alpha,\beta}.$$

7. Remarks and examples

The assumption that ρ is absolutely irreducible was not used in Sections 1–4, however, it is very useful for practical algorithms for writing ρ over $\mathbb{F}$. If ρ is reducible, then one may need to solve linear systems to find D satisfying Eq. (9), and the solution spaces may

be more than one-dimensional. Finding C from D is likely to be problematic. If ρ is irreducible but not absolutely irreducible, then the MEATAXE [8, 13] may be used to find D. In this case, however, the arithmetic needed to solve for μ (and hence find C) takes place in the division algebra $\mathrm{End}(\rho)$ of matrices commuting with $\rho(\mathfrak{A})$. See [5] for a description of some of the relevant noncommutative theory. We shall assume henceforth that $\mathfrak{A} = \mathbb{F}H$ is a group algebra.

The connection between $\mathbb{E}H$-modules and $\mathbb{F}H$-modules is clarified by considering normal bases. The following simple observation is not made explicitly in texts covering modular representation theory such as [7]. Let $(\alpha(\lambda))_{\alpha\in G}$ be a normal basis for $\mathbb{E}$ over $\mathbb{F}$. Let $V = \mathbb{E}^{d\times 1}$ and $U = \mathbb{F}^{d\times 1}$. Then V viewed as an $\mathbb{F}H$-module is a direct sum of $|G|$ Galois conjugate $\mathbb{F}H$-submodules: $V = \dot{+}_{\alpha\in G}\alpha(\lambda)U$. Note that $A^{-1}\rho(h)A \in \mathrm{GL}_d(\mathbb{F})$ for $h \in H$ and so

$$\alpha(\lambda)UA^{-1}\rho(h)A = \alpha(\lambda)U = \alpha(\lambda U).$$

Thus the $\alpha(\lambda)U$ are $A^{-1}\rho A$ invariant, and Galois conjugate.

In the examples below $\mathbb{E} = \mathbb{F}(\zeta_n)$ is a subfield of the complex numbers, and $\zeta_n = e^{2\pi i/n}$. An automorphism α of $\mathbb{E}$ is determined by a number k satisfying $\alpha(\zeta_n) = \zeta_n^k$ and $\gcd(k,n) = 1$. As usual, $\mathbb{Q}$ denotes the rational field.

Example 1. Let H be the dicyclic group of order $8n$

$$H = \langle a, b \mid a^2 = b^{2n}, b^{4n} = 1, a^{-1}ba = b^{-1}\rangle.$$

Let $\mathbb{E} = \mathbb{Q}(\zeta)$ where $\zeta = \zeta_{4n}$. Define $\alpha \in \mathrm{Aut}(\mathbb{E})$ by $\alpha(\zeta) = \zeta^{-1}$. Then α has order 2, and $\mathbb{F} = \mathbb{E}^{\langle\alpha\rangle} = \mathbb{Q}(\zeta + \zeta^{-1})$. Define $\rho\colon H \to \mathrm{GL}_2(\mathbb{E})$ by

$$\rho(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad \rho(b) = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}.$$

Then $D_\alpha = \rho(a)$ and $D_1 = \rho(1)$ satisfies Eq. (9). Since $N_{\langle\alpha\rangle}(D_\alpha)$ equals $D_\alpha\alpha(D_\alpha) = D_\alpha^2 = -I$, it follows that $\lambda_\alpha = -1$. Since α is complex conjugation, $N_{\langle\alpha\rangle}(\mu_\alpha) = \mu_\alpha\overline{\mu_\alpha} = ||\mu_\alpha||^2 \geq 0$, so $N_{\langle\alpha\rangle}(\mu_\alpha) = -1$ has no solution. Consequently, ρ can not be written over $\mathbb{F}$.

Example 2. Let $H = \langle a, b \mid a^2 = b^{4n}, b^{8n} = 1, a^{-1}ba = b^{1+4n}\rangle$ and let $\mathbb{E} = \mathbb{Q}(\zeta)$ where $\zeta = \zeta_{8n}$. Define $\alpha \in \mathrm{Aut}(\mathbb{E})$ by $\alpha(\zeta) = \zeta^{1+4n} = -\zeta$. Then α has order 2, and $\mathbb{F} = \mathbb{E}^{\langle\alpha\rangle} = \mathbb{Q}(\zeta^2)$. Define $\rho\colon H \to \mathrm{GL}_2(\mathbb{E})$ by

$$\rho(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad \rho(b) = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{1+4n} \end{pmatrix}.$$

Set $D_1 = \rho(1)$ and $D_\alpha = \rho(a)$. Then $N_{\langle\alpha\rangle}(D_\alpha) = -I$, so $\lambda_\alpha = -1$. Now $\mu_\alpha = \zeta^{2n}$ satisfies $N_{\langle\alpha\rangle}(\mu_\alpha) = \mu_\alpha^2 = -1 = \lambda_\alpha^{-1}$. Thus $C_1 = \rho(1)$

and $C_\alpha = \zeta^{2n}\rho(a)$. The matrix

$$A := \Pi_C\left(\frac{1+\zeta}{2}I\right) = \frac{1}{2}\begin{pmatrix} 1+\zeta & \zeta^{2n}(1-\zeta) \\ -\zeta^{2n}(1-\zeta) & 1+\zeta \end{pmatrix}$$

has $\det(A) = \zeta \neq 0$, and hence writes ρ over $\mathbb{F}$. If $\rho' = A^{-1}\rho A$, then

$$\rho'(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad \rho'(b) = \frac{1}{2}\begin{pmatrix} 1+\zeta^2 & \zeta^{2n}(1-\zeta^2) \\ \zeta^{2n}(1-\zeta^2) & -1-\zeta^2 \end{pmatrix}.$$

The similarity between A and $\rho'(b)$ is interesting. For each n there are many choices for μ_α, and then many choices for ν such that $\Pi_C(\nu I)$ is invertible. Our choices $\mu_\alpha = \zeta^{2n}$, $\nu = (1+\zeta)/2$ give a simple expression for $\rho'(b)$. Another choice when n is odd is $\mu_\alpha = 1+\zeta^n-\zeta^{3n}$ and $\nu = 1$.

Example 3. Let $H = \langle a, b \mid a^m = b^n = 1, a^{-1}ba = b^r\rangle$ where r is the order of m modulo n. Let $\zeta = \zeta_n$, $\mathbb{E} = \mathbb{Q}(\zeta)$, and let $\mathbb{F} = \mathbb{E}^{\langle\alpha\rangle}$ where $\alpha \in \mathrm{Aut}(\mathbb{E})$ is defined by $\alpha(\zeta) = \zeta^r$. Define $\rho\colon H \to \mathrm{GL}_m(\mathbb{E})$ by

$$\rho(a) = \begin{pmatrix} 0 & 1 & 0 & \\ & & \ddots & \\ 0 & 0 & & 1 \\ 1 & 0 & & 0 \end{pmatrix} \quad \text{and} \quad \rho(b) = \begin{pmatrix} \zeta & & & \\ & \zeta^r & & \\ & & \ddots & \\ & & & \zeta^{r^{m-1}} \end{pmatrix}.$$

Then $C_\alpha = \rho(a)$ and $C_{\alpha^i} = C_\alpha \alpha(C_\alpha)\cdots\alpha^{i-1}(C_\alpha) = \rho(a)^i$ and

$$A = \Pi_C(\lambda I) = \sum_{i=0}^{m-1} C_\alpha^i \alpha^i(\lambda) = (\alpha^{i-j}(\lambda))$$

is invertible if and only if λ defines a normal basis for $\mathbb{E}$ over $\mathbb{F}$. If $\rho' = A^{-1}\rho A$, then $\rho'(a) = \rho(a)$ and the expression for $\rho'(b)$ is rather complicated, and depends on r.

Example 4. Let $\mathbb{E} : \mathbb{F}$ be a finite Galois extension with group G. Let σ be the left regular representation $G \to \mathrm{Sym}(G)$ satisfying $\sigma_\alpha(\gamma) = \alpha\gamma$ and $\sigma_{\alpha\beta} = \sigma_\alpha \circ \sigma_\beta$. Let H be the split extension of $\mathbb{E}^\times$ by G. Specifically, let $H = G \times \mathbb{E}^\times$ where

$$(\alpha, \lambda)(\beta, \mu) = (\alpha\beta, \beta(\lambda)\mu) \qquad (\alpha, \beta \in G, \lambda, \mu \in \mathbb{E}^\times).$$

Define $\rho\colon H \to \mathrm{GL}_{|G|}(\mathbb{E})$ by $\rho(\alpha, \lambda) = (\eta(\lambda)\delta_{\sigma_\alpha(\eta),\eta})$ where $(\delta_{\xi,\eta})$ is the identity matrix. The (ξ, η) entry of $\rho(\alpha, \lambda)$ is zero unless $\xi = \sigma_\alpha(\eta)$ in which case it equals $\eta(\lambda)$. The (ξ, η) entry of $\rho(\alpha, \lambda)\rho(\beta, \mu)$ is zero unless $\xi = \sigma_{\alpha\beta}(\eta)$ in which case it equals $\sigma_\beta(\eta)(\lambda)\eta(\mu) = \eta(\beta(\lambda)\mu)$. This proves that ρ is a homomorphism. Since ρ is induced from a 1-dimensional representation $\mathbb{E}^\times \to \mathrm{GL}_1(\mathbb{E})$ which is fixed only by the identity automorphism, it follows from Clifford's theorem that ρ is absolutely irreducible. We may take C_α to be the permutation matrix

$\rho(\alpha,1)$ corresponding to σ_α. Then $A=\Pi_C(\lambda I)$ is invertible if and only if λ defines a normal basis for $\mathbb{E}$ over $\mathbb{F}$. If $|\mathbb{F}|=q$ and $|\mathbb{E}|=q^n$, then the probability that $\Pi_C(\lambda I)$ is invertible is $q^{-n}\sum_{d|n}\mu(n/d)q^d$ where μ denotes the Möbius function. It follows by considering base-q expansions that $\sum_{d|n}\mu(n/d)q^d\geq q^n-q^{n/p}\geq q^n-q^{n/2}$ where p is the smallest prime divisor of n. Hence $q^{-n}\sum_{d|n}\mu(n/d)q^d\geq 1-q^{-n/2}$.

References

[1] H. Brückner, Algorithmen für endliche auflösbare Gruppen und Anwendungen. PhD thesis, Aachner Beiträge zur Mathematik **22**, RWTH Aachen, 1998.

[2] C. Fieker, Über relative Normgleichungen in algebraichen Zahlkörper. PhD thesis, Techniche Univ. Berlin, 1997.

[3] H. Cohen, *A Course in Computational Algebraic Number Theory* (Graduate Texts in Mathematics **138**, Springer-Verlag, Berlin, 1993). MR1228206

[4] S.P. Glasby, R.B. Howlett, Writing representations over proper sub-fields, *Comm. Algebra* **25** (1997), no. 6, 1703–1712. MR 97a:20012

[5] S.P. Glasby, Modules induced from a normal subgroup of prime index, in: *Lecture Notes in Pure and Applied Mathematics* (to appear).

[6] P.R. Halmos, *Linear Algebra Problem Book* (Dolciani Mathematical Expositions **16**, Mathematical Association of America, 1995).

[7] B. Huppert, N. Blackburn, *Finite Groups II* (Springer, Berlin, 1982).

[8] D.F. Holt, S. Rees, Testing modules for irreducibility, *J. Austral. Math. Soc. Ser. A* **57** (1994), no. 1, 1–16. MR 95e:20023

[9] T.Y. Lam, A. Leroy, Hilbert 90 theorems over division rings, *Trans. Amer. Math, Soc.* **345** (1994), 595–622. MR1181184

[10] S. Lang, *Algebra*, Addison Wesley, 1965.

[11] P. Nuss, Noncommutative descent and nonabelian cohomology, *K-theory* **12** (1997), 23-74. MR1466623

[12] R.A. Parker, The computer calculation of modular characters (the meat-axe), in: *Computational Group Theory, Durham, 1982* (Academic Press, London, 1984), pp. 267–274. MR0760660

[13] R.A. Parker, An integral meataxe, in: *The Atlas of Finite Groups Ten Years On*, London Math. Soc. Lect. Notes **249** (1998), pp. 215–228. MR1647424

[14] S. Roman, *Field Theory* (Graduate Texts in Mathematics, vol. 158, Springer-Verlag, 1995). MR1329733

[15] P. Samuel, *Algebraic Theory of Numbers* (Herman, Paris, 1971). Translated from the French by A.J. Silberger. MR0265266

[16] J.-P. Serre, *Corps Locaux* (Hermann, Paris, 1968). MR0354618

[17] D. Simon, Solving norm equations in relative number fields using S-units, *Math. Comp.* **71** (2002), no. 239, 1287–1305. MR1898758

Department of Mathematics
Central Washington University
WA 98926-7424, USA
GlasbyS@cwu.edu